PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 133, Number 10, Pages 2873–2881
S 0002-9939(05)07921-9
Article electronically published on April 20, 2005

DENSITIES OF QUARTIC FIELDS WITH EVEN GALOIS GROUPS

SIMAN WONG

(Communicated by Wen-Ching Winnie Li)

ABSTRACT. Let $N(d,G,X)$ be the number of degree d number fields K with Galois group G and whose discriminant D_K satisfies $|D_K| \leq X$. Under standard conjectures in diophantine geometry, we show that $N(4,A_4,X) \ll_\epsilon X^{2/3+\epsilon}$, and that there are $\ll_\epsilon N^{3+\epsilon}$ monic, quartic polynomials with integral coefficients of height $\leq N$ whose Galois groups are smaller than S_4, confirming a question of Gallagher. Unconditionally we have $N(4,A_4,X) \ll_\epsilon X^{5/6+\epsilon}$, and that the 2-class groups of almost all Abelian cubic fields k have size $\ll_\epsilon D_k^{1/3+\epsilon}$. The proofs depend on counting integral points on elliptic fibrations.

1. INTRODUCTION

Given a transitive subgroup G of the symmetric group S_d, denote by $N(d,G,X)$ the number of degree d number fields K with Galois group G and whose discriminant D_K satisfies $|D_K| \leq X$. Questions about asymptotic properties of $N(d,G,X)$ naturally arise in connection with tabulation of number fields of a given degree and Galois type. This quantity is also closely related to questions about p-rank of class groups of number fields ([12], [22]). Given any such pair (d,G), Malle [14] recently conjectured that there exist constants $e(d,G) > 0, c(d,G) > 0$ and $v(d,G) \geq 0$, such that

$$N(d,G,X) \overset{?}{\sim} c(d,G)X^{e(d,G)} \log^{v(d,G)} X \quad \text{as } X \to \infty. \tag{1.1}$$

Malle also proposed an explicit formula for $e(d,G)$. When G is Abelian, this is a theorem of Wright [23]. A deep theorem of Davenport and Heilbronn [5] says that (1.1) holds for the pair $(3,S_3)$ with $e(3,S_3) = 1$. The recent work of Cohen *et al.* [4, p. 89] gives $e(4,D_4) = 1$ (where D_4 is the dihedral group of order 8). Malle also put forth the weaker conjecture[1]

$$X^{e(d,G)} \overset{?}{\ll}_{d,G} N(d,G,X) \overset{?}{\ll}_{\epsilon,d,G} X^{e(d,G)+\epsilon},$$

which for the pair $(4,S_4)$ has recently been proved independently by Yukie [24] and Bhargava [2], with $e(4,S_4) = 1$. See [4] for an excellent survey of these results.

Received by the editors March 11, 2004 and, in revised form, June 7, 2004.

2000 *Mathematics Subject Classification.* Primary 11G05; Secondary 11G35, 11R16, 11R29.

Key words and phrases. Class groups, discriminants, elliptic curves, elliptic fibrations, Galois groups, integral points, quartic fields.

The author was supported in part by NSA grant H98230-05-1-0069.

[1]Any O-constant in this paper depends only on those quantities (if any) adorning the corresponding $\ll$-sign.

Theorem 1.1. *Assume the ABC Conjecture, the Birch-Swinnerton-Dyer Conjecture and the Generalized Riemann Hypothesis for the L-functions of elliptic curves over* $\mathbf{Q}$*. Then*

$$N(4, A_4, X) \ll_\epsilon X^{2/3+\epsilon}.$$

Unconditionally we have

$$N(4, A_4, X) \ll_\epsilon X^{5/6+\epsilon}.$$

Baily [1] showed that $X^{1/2} \ll N(4, A_4, X) \ll X \log^4 X$. In [21] we improved this upper bound to $\ll_\epsilon X^{7/8+\epsilon}$. In general, Schmidt [18] showed that the number of degree d fields K with $|D_K| \leq X$ is $\ll_d X^{\frac{d+2}{4}}$. Theorem 1.1 says that conditionally, the exponent $e(4, A_4)$, if it exists, is $\leq 2/3 + \epsilon$ for every $\epsilon > 0$. Cohen *et al.* conjectured that $e(4, A_4) = 1/2$ and with an explicit value for $c(4, A_4)$; cf. [4, p. 90].

To prove Theorem 1.1, we first employ an inequality of Hunter to convert the problem of counting quartic fields of discriminant $\leq X$ and with even Galois groups, to counting quartic polynomials f whose coefficients a_i are bounded in terms of X and with $\mathrm{disc}(f)$ being a square. In other words, we want to count integral points on the hypersurface $y^2 = \mathrm{disc}(f)$ with the a_i bounded in terms of X; we do that by mapping this hypersurface to an elliptic threefold and then count points fiberwise. Geometrically speaking, we construct a coarse moduli space for these quartic fields, and then exploit the geometry of this space to get non-trivial estimates. In their recent work, Ellenberg and Venkatesh [9] improve Schmidt's estimate for large d. Their construction can be thought of as putting a level structure on this moduli space, and their main result follows by carefully controlling the size of the fiber of the map from this fine moduli space to our coarse moduli space. The proofs in [9] turn out to make relatively little use of the geometry of this fine moduli space; it would be interesting to see if we can get better results by combining our explicit geometric analysis with this general construction.

Heilbronn [12] showed that given an Abelian cubic field k with h_k^* order 2 elements in its class group Cl_k, there exist exactly $\frac{1}{3}h_k^*$ quadruples of conjugate A_4 quartic fields of discriminant D_k whose Galois closure contains k. Combining this with Theorem 1.1 and recalling that there are $\gg\ll X^{1/2}$ Abelian cubic fields of discriminant $\leq X$, we get the following result which improves on average [21, Thm. 1].

Corollary 1.2. *Under the same hypotheses as in Theorem* 1.1*, as k runs through all Abelian cubic fields, we have*

$$\sum_{D_k \leq X} h_k^* \ll_\epsilon X^{2/3+\epsilon}.$$

In particular, for almost all k the elementary 2-subgroup of Cl_k has size $\ll_\epsilon D_k^{1/6+\epsilon}$. Unconditionally, the same results hold with the exponent $2/3+\epsilon$ and $1/6+\epsilon$ by $5/6+\epsilon$ and $1/3+\epsilon$, respectively. □

There is a unique equivalent class of embedding of A_4 into $PGL_2(\mathbf{C})$, so the Galois closure L of an A_4 quartic field K gives rise to a unique projective representation $\tilde{\rho}_L : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to PGL_2(\mathbf{C})$. Tate showed that $\tilde{\rho}_L$ has a unique lift to an ordinary representation $\rho_L : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\mathbf{C})$ with minimal Artin conductor $=: N_L$, and Langlands showed that ρ_L comes from an automorphic form on $GL(2)$

(not necessarily holomorphic) of conductor N_L. Such ρ_L and the associated automorphic form are called *tetrahedral*. In [21] we showed that $N_L \ll D_K$. Invoke Theorem 1.1 and we get the following result.

Corollary 1.3. *Under the same hypotheses as in Theorem* 1.1*, there are* $\ll_\epsilon X^{2/3+\epsilon}$ *tetrahedral automorphic forms of conductor* $\leq X$ *coming from Artin representations.* □

Michel-Venkatesh [16] showed that unconditionally there are $\ll_\epsilon N^{2/3+\epsilon}$ tetrahedral forms of level N and with a given Nebentypus. Corollary 1.3 improves *on average* this upper bound among those tetrahedral forms which come from Artin representations and with no restriction on the Nebentypus. The Langlands program predicts that *every* tetrahedral form comes from Artin representations; for holomorphic forms this is due to Deligne-Serre [6].

We now discuss another way to count number fields, namely by way of their generating polynomials. Van der Waerden [20] showed that almost all monic, degree $d > 1$ polynomials with integer coefficients, as ordered by their height (:= maximum of the absolute value of their coefficients), are irreducible and have Galois group S_d. Gallagher [10] refined this by showing that

$$\begin{aligned} E_d(N) \quad := \quad & \text{set of monic, degree } d > 1 \text{ polynomials of height} \\ & \leq N \text{ whose the Galois group is smaller than } S_d \end{aligned}$$

satisfies

$$\#E_d(N) \ll_d N^{d-1/2} \log N. \tag{1.2}$$

Dörge [7] showed that there are $\gg_\epsilon N^{d-1-\epsilon}$ reducible polynomials of height $\leq N$, and Gallagher asked if we can sharpen (1.2) to $\ll_{d,\epsilon} N^{d-1+\epsilon}$. Our technique here yields the following conditional improvements.

Theorem 1.4. *Under the same hypotheses as in Theorem* 1.1*, for every* $\epsilon > 0$ *we have*

$$\#E_4(N) \ll_\epsilon N^{3+\epsilon} \quad \textit{and} \quad \#\{f \in E_5(N) : \operatorname{disc}(f) \textit{ is a square}\} \ll_\epsilon N^{4+\epsilon}.$$

Our approach via integral points does not take into account the reducible polynomials (nor did Gallagher's sieve argument). This brings up a natural question: what is the true order of magnitude of $\#\{f \in E_d(N) : f \text{ is irreducible}\}$? To the best of our knowledge, explicit constructions in the literature (e.g. [17]) only give $\ll_\epsilon N^{1+\epsilon}$ quartic polynomials of height $\leq N$ with A_4 Galois group; and the trinomials $x^4 + ax^2 + b$ give $(1 + o(1))N^2$ D_4-quartics of height $\leq N$. Also, our estimate for $\#E_4(N)$ does *not* contradict the theorem of Cohen *et al.* on $N(4, D_4, X)$; cf. Remark 5.1.

2. S-integral points

Recall that the height $ht(r)$ of a reduced fraction $r = a/b$ is $\max(|a|, |b|)$. Also, recall our convention for O-constants.

Lemma 2.1. *Let* $f = a_0x^d + \cdots + a_d \in \mathbf{Q}[x]$ *be separable with* $d = 3$ *or* 4*. Suppose that*

(i) $ht(a_i) \leq X$ *for all* i*,*
(ii) *the denominator of every* a_i *has absolute value* $\leq B$*, and*
(iii) $ht(a_0) \leq B$*.*

Then under the same hypotheses as in Theorem 1.1*, there are* $\ll_{\epsilon,B} X^{\epsilon}$ *integral points for the equation* $y^2 = f(x)$ *with* $|x| \ll X$*.*

Proof. First, suppose f is cubic. Denote by $E/\mathbf{Q}$ the elliptic curve defined by

$$y^2 = f(x). \tag{2.1}$$

If we write $c_4(E)$ and $c_6(E)$ for the usual quantities [19, p. 46] associated to the (not necessarily minimal) Weierstrass equation (2.1), conditions (i) and (iii) imply that the *rational numbers* $c_4(E), c_6(E)$ satisfy

$$|c_4(E)| \ll X^2, \ |c_6(E)| \ll X^3. \tag{2.2}$$

Thanks to condition (ii), the conductor of $E/\mathbf{Q}$, which is an *integer*, satisfies $\ll_B |c_4(E)^3 - c_6(E)^2| \ll X^6$. Under BSD and GRH, it then follows from the work of Mestre [15] that

$$(\text{the Mordell-Weil rank of } E/\mathbf{Q}) \ll_B \log X/\log\log X.$$

Denote by

$$E' : \overline{y}^2 = \overline{x}^3 + \overline{A}\overline{x} + \overline{B} \tag{2.3}$$

a quasi-minimal model [19, Exer. 8.14(c)] of $E/\mathbf{Q}$, i.e. $|4\overline{A}^3 + 27\overline{B}^2|$ is minimized among all models (2.3) of E subject to $\overline{A}, \overline{B} \in \mathbf{Z}$. To convert (2.1) to E' we use a linear change of variables

$$x = u^2\overline{x} + r, \ \ y = u^3\overline{y} + u^2 s\overline{x} + t$$

with $u, s, t \in \mathbf{Z}, u \neq 0$ (cf. [19, p. 49]). This transformation takes the integral points on (2.1) to (a subset of the) S'-integral points on E', where S' is the set of prime divisors of u. In light of (2.2), we have $u \ll_B X^{1/2}$, whence

$$\#S' \ll_B \log X/\log\log X.$$

Finally, assume the ABC conjecture. Then Hindry-Silverman [13] showed that there exist absolute constants $c, \sigma > 0$ so that

$$\begin{aligned} \#(\text{integral points on (2.1)}) &\leq \#(S'\text{-integral points on } E') \\ &\ll_B c^{\#S' + (1+\operatorname{rank}(E/\mathbf{Q}))\sigma} \quad \text{by [13, Thm. 0.7]} \\ &\ll_B c_0^{\log X/\log\log X} \end{aligned}$$

for some absolute constant $c_0 > 0$, as desired.

Next, suppose f is quartic. If (2.1) has no integral points (x, y) with $|x| \ll X$, then we are done, so suppose otherwise. To bring (2.1) to the form $y^2 = x^3 + \alpha x + \beta$ we use a projective change of coordinates to move P to ∞; in doing so the new coefficients α, β are now rational functions of *bounded degree* in the coefficients of (2.1) and in the coordinates of P. Proceed as in the cubic case and we see that

- under BSD and GRH, this elliptic curve has conductor $\ll_B \log X/\log\log X$; and
- upon fixing a quasi-minimal model E' of this curve, the integral points of (2.1) now correspond to (a subset of the) S'-integral points on E', with $S' \ll_B \log X/\log\log X$.

It then follows as before that under ABC, (2.1) has $\ll_{\epsilon,B} X^{\epsilon}$ integral points, as desired. □

3. Hunter's inequality

Let $K/\mathbf{Q}$ be an extension of degree d. According to the Hunter inequality [3, Theorem 6.4.2], there exists an algebraic integer $\theta_K \in K - \mathbf{Q}$ such that, upon writing $\theta_K^{(1)}, \dots, \theta_K^{(d)}$ for the Galois conjugates of θ_K, we have

$$\sum_{i=1}^{d} |\theta_K^{(i)}|^2 \ll_d |D_K|^{1/(d-1)} \quad \text{and} \quad 0 \le \sum_{i=1}^{d} \theta_K^{(i)} \le d/2. \tag{3.1}$$

Denote by $x^d + a_1(\theta_K)x^{d-1} + \cdots + a_d(\theta_K) \in \mathbf{Z}[x]$ the minimal polynomial of θ_K over $\mathbf{Q}$. It follows that

$$0 \le a_1(\theta_K) \le d/2 \quad \text{and} \quad |a_j(\theta_K)| \ll_d |D_K|^{\frac{j}{2(d-1)}} \quad \text{if } j > 1.$$

Under the change of variable $x = (z - a_1(\theta_K))/d$ we get another defining polynomial $z^d + a_2'(\theta_K)z^{d-2} + \cdots + a_d'(\theta_K) \in \mathbf{Z}[z]$ of the same field $\mathbf{Q}(\theta_K)$ with

$$|a_j'(\theta_K)| \ll_d |D_K|^{\frac{j}{2(d-1)}} \quad \text{if } j > 1. \tag{3.2}$$

If $K/\mathbf{Q}$ is a primitive extension, i.e. there are no non-trivial intermediate extensions between $\mathbf{Q}$ and K, then necessarily $K = \mathbf{Q}(\theta_K)$. Thus the number of *primitive*, degree d fields K with $|D_K| \le X$ is bounded by the number of monic, degree d integer polynomials whose coefficients satisfy the bounds (3.2). In particular, there are

$$\ll_d X^{\frac{2}{2(d-1)} + \cdots \frac{d}{2(d-1)}} = X^{\frac{d+2}{4}}$$

such fields. Note that this is of the same order of magnitude as Schmidt's estimate. This should not be surprising, since both Hunter and Schmidt relied on techniques from geometry of numbers. Now, there is a version of Hunter's inequality for relative extensions. It seems likely that this relative version will allow us to inductively derive Schmidt's estimate in full generality (Schmidt also argued by induction). We will not make use of Schmidt's estimate, so we will not pursue this topic further.

4. Quartic fields

Proof of Theorem 1.1. Quartic fields with A_4 Galois groups are necessarily primitive. By our discussion in section 3 it suffices to count quartic polynomials

$$f_4(x) = x^4 + a_2x^2 + a_3x + a_4$$

whose coefficients satisfy the quartic Hunter bounds

$$|a_j| \ll X^{j/6} \quad (2 \le j \le 4) \tag{4.1}$$

and for which

$$\operatorname{disc}(f_4) = 256a_4^3 - 128a_2^2a_4^2 + (16a_2^4 + 144a_2a_3^2)a_4 - 4a_2^3a_3^2 - 27a_3^4 \tag{4.2}$$

is a square. Note that a_3 occurs in even powers only, so we can view

$$Y : y^2 = \operatorname{disc}(f_4) \tag{4.3}$$

as an affine threefold in (a_2, a_3, a_4, y) that double covers the affine cubic threefold

$$W : y^2 = 256a_4^3 - 128a_2^2a_4^2 + (16a_2^4 + 144a_2w)a_4 - 4a_2^3w - 27w^2. \tag{4.4}$$

According to Maple, the *affine* singular locus of W is

$$\Sigma : \ \Big\{(a_2, a_4, y, w) : a_4 = \frac{-a_2^2}{12},\ w = \frac{-8a_2^3}{27},\ y = 0\Big\}.$$

So if we pick a point $P = (a_2, a_4, y, w) \in \Sigma$, then any line defined over $\mathbf{Q}(a_2)$ which is not contained in W and passes through P will intersect W at one more point defined over $\mathbf{Q}(a_2)$. This defines a $\mathbf{Q}(a_2)$-birational map from the *affine* variety $W_{\mathbf{Q}(a_2)}$ to $\mathbf{A}^2_{\mathbf{Q}(a_2)}$. To count integral points on (4.3) that satisfy the Hunter bounds (4.1), we first enumerate integral points on W by making explicit this birational map $W_{\mathbf{Q}(a_2)} \dashrightarrow \mathbf{A}^2_{\mathbf{Q}(a_2)}$, and then counting those whose w-coordinate is a square; the latter problem turns out to involve counting integral points on elliptic curves.

We begin by constructing the birational map. Over the function field $\mathbf{Q}(a_2)$ the affine singular locus Σ becomes a singular *point*, and our first step is to move this point to the origin via the change of variables $a_4 = \overline{a_4} - a_2^2/12, w = \overline{w} - 8a_2^3/27$. This turns (4.4) into

$$y^2 - 256\overline{a_4}^3 + 192a_2^2\overline{a_4}^2 - 144a_2\overline{a_4 w} + 27\overline{w}^2 = 0. \tag{4.5}$$

Next, we blow up the origin on this affine coordinate patch, via the change of variables

$$\overline{a_4} = tA, \;\; y = tB, \;\; \overline{w} = tC.$$

This turns (4.5) into

$$t^2(B^2 - 256tA^3 + 192A^2a_2^2 - 144a_2AC + 27C^2) = 0. \tag{4.6}$$

Solving t from the second factor in (4.6) (the proper transform of the blowup), we get

$$t = (B^2 + 3(8a_2A - 3C)^2)/(256A^3). \tag{4.7}$$

Unwind all the change of variables and we see that

$$a_4 = tA - a_2^2/12, \quad y = tB, \quad a_3^2 = tC - 8a_2^3/27. \tag{4.8}$$

The correspondence $(a_3, a_4, w) \mapsto [A : B : C]$ is the desired birational map $W_{\mathbf{Q}(a_2)} \dashrightarrow \mathbf{A}^2_{\mathbf{Q}(a_2)}$. In particular, given an integral point (a_2, a_3, a_4, y) on (4.3), we can take (A, B, C) above to be integers with $\gcd(A, B, C) = 1$ and $t \in \mathbf{Q}$.

Lemma 4.1. *Let (A, B, C) be an integer triple coming from (a_2, a_3, a_4, w) as above. Then $64A^3$ divides $B^2 + 3(8a_2A - 3C)^2$.*

Proof. Denote by $d(r)$ the denominator of a reduced, non-zero fraction r.

Both a_2 and $a_4 = tA - a_2^2/12$ are integers, so $d(tA)$ divides 12. But $A \in \mathbf{Z}$ and $t = n/(256A^3)$ with $n := B^2 + 3(8a_2A - 3C)^2$, so $d(n/64A^3)$ divides $3A$. In particular, A divides $(B^2 + 27C^2)$. This plus $\gcd(A, B, C) = 1$ means that $\gcd(A, C) = 1$.

Since $a_3^2 = tC - 8a_2^3/27$ is an integer, $d(tC)$ divides 27. Combined with $\gcd(A, C) = 1$, $d(n/64A^3) \mid 3A$ and $tC = (c/4)(n/64A^3)$, this means $d(n/64A^3)$ divides 3. It then follows from $a_3^2 = tC - 8a_2^3/27 \in \mathbf{Z}$ that tC is in fact an integer. Going back one step, that means $d(n/64A^3) = 1$, i.e. $64A^3$ divides n, as desired. □

Note that $B^2 + 3(8a_2A - 3C)^2$ is a norm form in $\mathbf{Q}(\sqrt{-3})$. So if a prime $p \equiv 2 \pmod 3$ divides A, then Lemma 4.1 says that p divides both B and $8a_2A - 3C$, and hence $\gcd(A, B, C) > 1$, a contradiction. So A is divisible *only* by primes $\equiv 1 \pmod 3$ and by 3. That means $A \in \mathbf{Z}$ is a norm from $\mathbf{Q}(\sqrt{-3})$; ditto for $4t$, thanks to Lemma 4.1. Thus we can write

$$A = \pm(\alpha^2 + 3\beta^2), \tag{4.9}$$

$$\frac{B^2 + 3(8a_2A - 3C)^2}{A^3} = \pm(\gamma^2 + 3\delta^2) \tag{4.10}$$

with $\alpha, \beta, \gamma, \delta \in \frac{1}{2}\mathbf{Z}$. Note that by (4.10), the $\pm$ signs in (4.9) and (4.10) are the same. Rewriting (4.10) as $B^2 + 3(8a_2A - 3C)^2 = \pm A^3(\gamma^2 + 3\delta^2)$ and eliminating A using (4.9), we get the equality of two norms from $\mathbf{Q}(\sqrt{-3})$. Comparing the real and imaginary parts, we get[2]

$$\pm B = \alpha^3\gamma - 9\alpha^2\beta\delta - 9\alpha\beta^2\gamma + 9\beta^3\delta, \tag{4.11}$$

$$8a_2A - 3C = \delta\alpha^3 + 3\gamma\beta\alpha^2 - 9\delta\beta^2\alpha - 3\gamma\beta^3. \tag{4.12}$$

Substitute these back into (4.8), we get

$$\begin{aligned} a_3^2 &= \frac{-8a_2^3}{27} \pm \frac{\gamma^2 + 3\delta^2}{3 \cdot 256}\Big(\pm 8a_2(\alpha^2 + 3\beta^2) \\ &\qquad - (\delta\alpha^3 + 3\gamma\beta\alpha^2 - 9\delta\beta^2\alpha - 3\gamma\beta^3)\Big), \end{aligned} \tag{4.13}$$

$$a_4 + \frac{a_2^2}{12} = \pm(\alpha^2 + 3\beta^2)(\gamma^2 + 3\delta^2). \tag{4.14}$$

Now, $(\alpha + \beta\sqrt{-3})(\gamma + \delta\sqrt{-3})$ is the product of two half-integers in $\mathbf{Q}(\sqrt{-3})$, and, by (4.14), this product has norm $\ll X^{2/3}$. There are $\ll X^{2/3}$ such products, and each one has $\ll_\epsilon X^\epsilon$ factorizations (the unit group of $\mathbf{Z}[\frac{1+\sqrt{-3}}{2}]$ is finite!). So all together there are $\ll_\epsilon X^{2/3+\epsilon}$ pairs of 4-tuples $(\alpha, \beta, \gamma, \delta)$ coming from (4.9) and (4.10).

View the right side of (4.13) as a cubic in a_2 and compute its discriminant using MAPLE. Then keeping in mind that the two $\pm$ signs are the same, we get

$$(\gamma^2 + 3\delta^2)^2(\alpha^3\gamma - 9\alpha^2\beta\delta - 9\alpha\beta^2\gamma + 9\beta^3\delta)^2/2^{10}3^6. \tag{4.15}$$

Recall (4.10) and (4.11) and we see that this is $(256tB)^2/2^{10}3^6$, which by (4.8) is $2^6y^2/3^6$. But $y^2 = \mathrm{disc}(f_4) \neq 0$. So for any 4-tuple $(\alpha, \beta, \gamma, \delta)$ coming from (4.9) and (4.10), the equation (4.13) always defines an elliptic curve over $\mathbf{Q}$ in a_2 and a_3. Lemma 2.1 then says that, conditionally, there are $\ll_\epsilon X^\epsilon$ integral points on this curve with $|a_2| \ll X^{2/6}$ and $|a_3| \ll X^{3/6}$. We saw that there are $\ll_\epsilon X^{2/3+\epsilon}$ such 4-tuples, so we get the conditional part of Theorem 1.1.

To get an unconditional estimate we use [11, Thm. 3]. First, make the change of variables $a_3 = a_3'/a_1'$ and $a_2 = a_2'/a_1'$ and dehomogenize (4.13) to get a cubic form $F(a_1', a_2', a_3')$. Apply [11, Thm. 3], specifically equation (1.18) there, with $B_1 = 1, B_2 = X^{1/3}, B_3 = X^{1/2}$ and we see that F has $\ll_\epsilon X^{1/6+\epsilon}$ integral points with $|a_i'| \ll B_i$. The unconditional form of Theorem 1.1 now follows. □

5. Counting polynomials

To prove Theorem 1.4 we proceed in two steps. First we count

$$E_d'(N) := \{f \in E_d(N) : \mathrm{disc}(f) \text{ is a square}\};$$

for that we pattern upon the proof of Theorem 1.1(b). To handle $E_4(N) - E_4'(N)$ we use Galois theory of quartic polynomials to identify this set with integral points on a different elliptic fibration, and then count points as before.

Step I: $E_4'(N)$ and $E_5'(N)$

We begin with the quartic case. We identify polynomials $f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$ in $E_4(N)$ with 4-tuples $(a_1, \ldots, a_4)$ with $|a_i| \leq N$. Mimicking the

[2]Such an equality only determines the real and imaginary parts up to sign; we pin down the signs in (4.12) by multiplying, if necessary, each of $\alpha, \beta, \gamma, \delta$ by -1.

argument in §4, we extract the first three coordinates of these 4-tuples to get triples $\mathbf{a}$ and then specialize the hypersurface $y^2 = \mathrm{disc}(f)$ at $\mathbf{a}$ to get (possible singular) cubic curves $E_{\mathbf{a}} : y^2 = \mathrm{disc}_{\mathbf{a}}(f)$. As before, we get conditionally $\ll_\epsilon N^{3+\epsilon}$ integral points on this hypersurface coming from 3-tuples $\mathbf{a} = (a_1, a_2, a_3)$ for which $E_{\mathbf{a}}$ is non-singular.

The singular triples are characterized by the vanishing of $\Delta :=$ the discriminant of $\mathrm{disc}(f)$, where f is viewed as a cubic polynomial in a_4. Note that Δ is a non-trivial polynomial in a_1, a_2 and a_3, since $\Delta_{a_1=a_2=0}$ is already non-trivial. So if we factor $\Delta = \Delta_1 \cdots \Delta_n$ into a product of $\mathbf{Q}$-irreducible polynomials, then there are $\ll N^2$ solutions $\mathbf{a} = (a_2, a_3, a_4)$ of height $\leq N$ for each $\Delta_i = 0$. For each such triple the equation $y^2 = \mathrm{disc}_{\mathbf{a}}(f)$ trivially has $\ll N$ solutions with $|a_4| \leq N$. Thus there are $\ll_\epsilon N^3$ 4-tuples corresponding to singular $E_{\mathbf{a}}$. All together, this gives $\#E_4'(N) \ll_\epsilon N^{3+\epsilon}$.

Next, take $g(x) = x^5 + b_1x^4 + \cdots + b_5 \in \mathbf{Z}[x]$. Then $\mathrm{disc}(g)$ is a quartic polynomial in b_5 with coefficients in $\mathbf{Z}[b_1, \cdots, b_4]$, so $y^2 = \mathrm{disc}(g)$ is now an elliptic fibration over a 4-dimensional base. Continue as in the quartic case and we get $\#E_5'(N) \ll_\epsilon N^{4+\epsilon}$.

Step II: $E_4(N) - E_4'(N)$

By Dörge there are $\ll N^{3+\epsilon}$ reducible polynomials in this set. Now, suppose $f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$ is irreducible over $\mathbf{Q}$. Then its Galois group has size < 12 if and only if the resolvent cubic

$$R_f(x) = x^3 - a_2x^2 + (a_1a_3 - 4a_4)x - a_1^2a_4 + 4a_2a_4 - a_3^2 \tag{5.1}$$

of f is reducible over $\mathbf{Q}$. Note that $R_f(x)$ is a Weierstrass equation in x and a_3 over $\mathbf{Z}[a_1, a_2, a_4]$, with discriminant

$$\Delta = a_4(-a_1^4 + 8a_1^2a_2 - 16a_2^2 + 64a_4)^2. \tag{5.2}$$

There are $\ll N^2$ triples (a_1, a_2, a_4) for which $\Delta = 0$ and with every $|a_i| \leq N$: for each of the two factors in (5.2), we can choose any a_1, a_2 and solve for a_4 accordingly. Given such a singular triple, (5.1) trivially has $\ll N$ solutions with $|a_3| \leq N$. For the remaining $\ll N^3$ triples (a_1, a_2, a_4) for which $\Delta \neq 0$, any rational root of (5.1) is an *integer* divisor of a_3^2, and hence it is $\leq N^2$; Lemma 2.1 then shows that (5.1) has $\ll_\epsilon N^\epsilon$ integral points. All together, we get $\#(E_4(N) - E_4'(N)) \ll_\epsilon N^{3+\epsilon}$. This completes the proof of Theorem 1.4.

Remark 5.1. Our argument leading to the estimate $\#(E_4(N) - E_4'(N)) \ll_\epsilon N^{3+\epsilon}$ does not contradict the result of Cohen *et al.* [4, p. 89] that $N(4, D_4, X) \sim c(4, D_4)X$. To see this, let us count $N(4, D_4, X)$ using this same technique, i.e. to count triples (a_2, a_3, a_4) that satisfy (5.1) plus the Hunter bounds (4.1). Repeat the calculation for Step II above and we see that $\Delta = 0$ for $\ll X^{2/6+3/6}$ such triples. For the remaining triples, as before, each elliptic curve (5.1) still has $\ll_\epsilon X^\epsilon$ integral points. The number of such curves is $\ll$ the number of pairs (a_2, a_4), which is $\ll X^{2/6+4/6}$, so all together there are $\ll_\epsilon X^{1+\epsilon}$ triples corresponding to D_4-quartic fields K with $|D_K| \leq X$. This is compatible with the result of Cohen *et al.*

Remark 5.2. If we try to bound $\#(E_5(N) - E_5'(N))$ as we did in Step II, we will arrive at a *sextic* in the extra variable A over $\mathbf{Z}[b_1, \ldots, b_5]$. Hold four of the b_i fixed and we get a curve of arithmetic genus 10. Provided that these curves have positive geometric genus, we can try to complete the argument by formulating a suitable form of the theorem of Hindry-Silverman plus a delicate analysis of the singular loci of this sextic.

Acknowledgment

I thank the referee for useful comments.

References

[1] A. M. Baily, On the density of discriminants of quartic fields. *J. Reine Angew. Math.* **315** (1980) 190-210. MR0564533 (81c:12006)
[2] M. Bhargava, Gauss composition and generalizations, in: *Proc. ANTS-V*, 1-8. Lect. Notes in Comp. Sci. 2369. Springer-Verlag, 2002. MR2041069
[3] H. Cohen, *A course in computational algebraic number theory*. Springer-Verlag, 1993. MR1228206 (94i:11105)
[4] H. Cohen, F. Diaz y Diaz and M. Olivier, A survey of discriminant counting, in: *Proc. ANTS-V*, 80-94. Lect. Notes in Comp. Sci. 2369. Springer-Verlag, 2002. MR2041075 (2005a:11173)
[5] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II. *Proc. Royal Soc. London. Ser. A* **322** (1971) 405-420. MR0491593 (58:10816)
[6] P. Deligne and J. P. Serre, *Formes modulaires de poids* 1. *Ann. Sci.École Norm. Sup.* **7** (1974) 507-530. MR0379379 (52:284)
[7] K. Dörge, Abschätzung der Anzahl der reduziblen Polynome. *Math. Ann.* **160** (1965) 59-63. MR0181638 (31:5865)
[8] J. S. Ellenberg, On the average number of octahedral modular forms. *Math. Res. Lett.* **10** (2003) 269-273. MR1981903 (2004b:11070)
[9] J. S. Ellenberg and A. Venkatesh, The number of extensions of a number field with fixed degree and bounded discriminant. xxx-NT preprint, Sept. 7, 2003.
[10] P. X. Gallagher, The large sieve and probabilistic Galois theory. *Proc. Symp. Pure Math.* v. 24. AMS (1973) 91-101. MR0332694 (48:11020)
[11] D. R. Heath-Brown, The density of rational points on curves and surfaces. *Ann. Math.* **155** (2002) 553-595. MR1906595 (2003d:11091)
[12] H. Heilbronn, On the 2-classgroup of cubic fields, in: *Studies in Pure Math.*, 117-119. Academic Press, London. 1971. MR0280461 (43:6181)
[13] M. Hindry and J. H. Silverman, The canonical height and integral points on elliptic curves. *Invent. Math.* **93** (1988) 419-450. MR0948108 (89k:11044)
[14] G. Malle, On the Distribution of Galois Groups. *J. Number Theory* **92** (2002) 315-329. MR1884706 (2002k:12010)
[15] J. F. Mestre, Formules explicites et minorations de conducteurs de variétés algébriques. *Compos. Math.* **58** (1986) 209-232. MR0844410 (87j:11059)
[16] P. Michel and A. Venkatesh, On the dimension of the space of cusp forms associated to 2-dimensional complex Galois representations. *IMRN* (2002) no. 38, 2021-2027. MR1925874 (2003i:11064)
[17] E. Nart and N. Vila, Equations with absolute Galois group isomorphic to A_n. *J. Number Theory* **16** (1983) 6-13. MR0693389 (85b:11081)
[18] W. M. Schmidt, Number fields of given degree and bounded discriminant. *Astérisque* **228** (1995) 189-195. MR1330934 (96e:11153)
[19] J. H. Silverman, *The arithmetic of elliptic curves*. Springer-Verlag, 1986. MR0817210 (87g:11070)
[20] B. L. van der Waerden, Die Seitenheit der reduziblen Gleichungen und der Gleichungen Affekt. *Monatsh. Math.* **43** (1936) 133-147.
[21] S. Wong, Automorphic forms on $GL(2)$ and the rank of class groups. *Crelle* **515** (1999) 125-153. MR1717617 (2000g:11042)
[22] S. Wong, On the rank of ideal class groups, in: *Proc. Fourth Canad. Number Theory Conf.*, 377-383. AMS, 1999. MR1684617 (2000k:11126)
[23] D. J. Wright, Distribution of discriminants of abelian extensions. *Proc. LMS* **58** (1989) 17-50. MR0969545 (90b:11115)
[24] A. Yukie, *Density theorems related to prehomogeneous vector spaces*. Preprint.

Department of Mathematics & Statistics, University of Massachusetts, Amherst, Massachusetts 01003-9305

E-mail address: siman@math.umass.edu